IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A network adapter system, comprising:

[[(a)]] a processor positioned on a network adapter coupled between an end-point computer and a network, the network adapter capable of being installed on the end-point computer;

[[(b)]] wherein the processor is adapted for virus scanning and content scanning of network traffic transmitted between the end-point computer and the network, the content scanning including scanning for unwanted content other than viruses;

[[(c)]] wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data;

[[(d)]] wherein the virus signature files are stored on non-volatile solid state memory on the network adapter;

[[(e)]] wherein the processor is ~~capable of being~~ user-configured;

[[(f)]] wherein the processor ~~is capable of determining~~determines whether received packets are of interest, ~~passing~~passes received packets that are not of interest to the end-point computer, and ~~scanning~~scans received packets that are of interest; wherein a predetermined amount of the received packets are assembled for determining whether the received packets are of interest, the received packets including packets received at the network adapter.

2. (Cancelled)

3. (Currently Amended) The network adapter system as recited in claim 1, wherein the processor is ~~capable of being~~ user-configured locally.

4. (Currently Amended) The network adapter system as recited in claim 1, wherein the processor ~~is capable of being~~ user-configured remotely via a network connection with the network adapter.

5. (Currently Amended) The network adapter system as recited in claim 1, wherein the processor ~~is capable of being~~ user-configured only after the verification of a password.

6. (Currently Amended) The network adapter system as recited in claim 1, wherein the manner in which the scanning is performed is ~~capable of being~~ user-configured.

7. (Currently Amended) The network adapter system as recited in claim 1, wherein the settings of the network adapter are ~~capable of being~~ user-configured.

8. (Cancelled)

9. (Previously Presented) The network adapter system as recited in claim 1, wherein the received packets are of interest based on an associated protocol.

10. (Cancelled)

11. (Cancelled)

12. (Currently Amended) The network adapter system as recited in claim 1, wherein the processor ~~is capable of denying~~denies received packets that fail the scan.

13. (Original) The network adapter system as recited in claim 1, wherein the scan is performed based on user settings.

14. (Currently Amended) A method for scanning network traffic on a network adapter, comprising:

[[(a)]] receiving packets at a network adapter including a processor positioned thereon. the network adapter ~~capable of being~~ installed on an end-point computer;

[[(b)]] virus scanning and content scanning of the packets utilizing the processor, the content scanning including scanning for unwanted content other than viruses; and

[[(c)]] conditionally taking security measures if the packets fail the scan;

[[(d)]] wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data;

[[(e)]] wherein the virus signature files are stored on non-volatile solid state memory on the network adapter;

[[(f)]] wherein the processor is ~~capable of being~~ user-configured;

[[(g)]] wherein the processor ~~is capable of determining~~determines whether received packets are of interest, ~~passing~~passes received packets that are not of interest to the end-point computer, and ~~scanning~~scans received packets that are of interest; wherein a predetermined amount of the received packets are assembled for determining whether the received packets are of interest, the received packets including packets received at the network adapter.

15. (Cancelled)

16. (Currently Amended) The method as recited in claim 14, wherein the processor is ~~capable of being~~ user-configured locally.

17. (Currently Amended) The method as recited in claim 14, wherein the processor is ~~capable of being~~ user-configured remotely via a network connection with the network adapter.

18. (Currently Amended) The method as recited in claim 14, wherein the processor is ~~capable of being~~ user-configured only after the verification of a password.

19. (Currently Amended) The method as recited in claim 14, wherein the manner in which the scanning is performed is ~~capable of being~~ user-configured.

20. (Currently Amended) The method as recited in claim 14, wherein the settings of the network adapter are ~~capable of being~~ user-configured.

21. (Cancelled)

22. (Previously Presented) The method as recited in claim 14, wherein the received packets are of interest based on an associated protocol.

23. (Cancelled)

24. (Cancelled)

25. (Currently Amended) The method as recited in claim 14, wherein the processor ~~is capable of denying~~denies received packets that fail the scan.

26. (Original) The method as recited in claim 14, wherein the scan is performed based on user settings.

27. (Currently Amended) A system for scanning network traffic on a network adapter, comprising:

[[(a)]] network adapter means for receiving packets, the network adapter means ~~capable of being~~ installed on an end-point computer;

[[(b)]] processor means positioned on the network adapter means for virus scanning and content scanning of the packets, the content scanning including scanning for unwanted content other than viruses; and

[[(c)]] means for conditionally taking security measures if the packets fail the scan;

[[(d)]] wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data;

[[(e)]] wherein the virus signature files are stored on non-volatile solid state memory on the network adapter means;

[[(f)]] wherein the processor means is ~~capable of being~~ user-configured;

[[(g)]] wherein the processor means ~~is capable of determining~~determines whether received packets are of interest, ~~passing~~passes received packets that are not of interest to the end-point computer, and ~~scanning~~scans received packets that are of interest;

wherein a predetermined amount of the received packets are assembled for determining whether the received packets are of interest, the received packets including packets received at the network adapter means.

28. (Currently Amended) A system for scanning network traffic on a network adapter, comprising:

[[(a)]] network adapter means for receiving packets, the network adapter means being installed on an end-point computer;

[[(b)]] logic positioned on the network adapter means for virus scanning and content scanning of the packets, the content scanning including scanning for unwanted content other than viruses; and

[[(c)]] logic for conditionally taking security measures if the packets fail the scan;

[[(d)]] wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data;

[[(e)]] wherein the virus signature files are stored on non-volatile solid state memory on the network adapter means;

[[(f)]] wherein the logic is ~~capable of being~~ user-configured;

[[(g)]] wherein the logic ~~is capable of determining~~determines whether received packets are of interest, ~~passing~~passes received packets that are not of interest to the end-point computer, and ~~scanning~~scans received packets that are of interest;

wherein a predetermined amount of the received packets are assembled for determining whether the received packets are of interest, the received packets including packets received at the network adapter means.

29. (Currently Amended) A network adapter system, comprising:

[[(a)]] a processor positioned on a network adapter coupled between an end-point computer and a network, the processor including a packet assembly module,

random access memory (RAM), and a scanner module. the network adapter being installed on the end-point computer;

[[(b)]] a user interface driver for identifying network traffic of interest transmitted between the end-point computer and the network;

[[(c)]] wherein the processor is adapted for discerning and virus scanning and content scanning of network traffic of interest transmitted between the end-point computer and the network, the content scanning including scanning for unwanted content other than viruses;

[[(d)]] wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data;

[[(e)]] wherein the virus signature files are stored on non-volatile solid state memory on the network adapter;

[[(f)]] wherein the network adapter receives the network traffic;

[[(g)]] wherein the processor is ~~capable of being~~ user-configured;

[[(h)]] wherein the processor ~~is capable of determining~~determines whether received network traffic is of interest, ~~passing~~passes received network traffic that is not of interest to the end-point computer, and ~~scanning~~scans received network traffic that is of interest;

wherein a predetermined amount of the received network traffic is assembled for determining whether the received network traffic is of interest, the received network traffic including network traffic received at the network adapter.

30. (Previously Presented) The network adapter system as recited in claim 1, wherein the content scanning enforces operational policies of an organization.

31. (Previously Presented) The network adapter system as recited in claim 30, wherein the policies include detecting entities selected from the group consisting of harassing content, pornographic content, junk e-mails, and misinformation.

32. (Cancelled)

33. (Previously Presented) The network adapter system as recited in claim 1, wherein the memory is user protected by configuring a network adapter BIOS with a password that only a user can change.

34. (Previously Presented) The network adapter system as recited in claim 1, wherein the received packets that are of interest include executable files.

35. (Previously Presented) The network adapter system as recited in claim 1, wherein the network adapter includes a Peripheral Component Interconnect (PCI) card.

36. (Previously Presented) The network adapter system as recited in claim 1, wherein the network adapter includes an Industry Standard Architecture (ISA) card.

37. (Previously Presented) The network adapter system as recited in claim 1, wherein the network adapter includes an Integrated Services Digital Network (ISDN) adapter.

38. (Previously Presented) The network adapter system as recited in claim 1, wherein the network adapter includes a cable modem adapter.

39. (Previously Presented) The network adapter system as recited in claim 1, wherein the network adapter includes a broadband adapter.

40. (Previously Presented) The network adapter system as recited in claim 1, wherein the unwanted content is selected from the group consisting of harassing content, pornographic content, junk e-mails, and misinformation.

41. (Previously Presented) The network adapter system as recited in claim 1, wherein the unwanted content includes harassing content, pornographic content, junk e-mails, and misinformation.

42. (Cancelled)

43. (Currently Amended) The network adapter system as recited in claim 1, wherein the received packets that are not of interest ~~to the end-point computer~~ bypass the scanning.

44. (New) The network adapter system as recited in claim 29, wherein the packet assembly module utilizes header information associated with received packets for assembling data fields of the received packets.

45. (New) The network adapter system as recited in claim 1, wherein if the received packets that are of interest fail the scanning, an alert is displayed which provides remedy options.

46. (New) The network adapter system as recited in claim 1, wherein scanning the received packets that are of interest is prioritized based on a file type associated with the received packets.